Amendments to the Claims:

1. (Currently Amended) A secured communication method for a mobile communications network, the method comprising:

receiving a request to provide a security key to a mobile device connected to the mobile communications network;

generating a unique security key for the requesting mobile device ~~using a public or private key mechanism unless the unique security key is preprogrammed into the mobile device~~ in response to receiving a unique identification number from the mobile device;

storing the unique security key in a first data ~~structure~~ storage mechanism in association with ~~the~~ a unique ~~value~~ identification number identifying the mobile device,

wherein the first data storage mechanism is accessible to a server system connected to the mobile device over a wide area communicatoin network, and wherein the first data storage mechanism is not directly accessible by the mobile device;

~~forwarding the unique security key to the mobile device;~~

~~storing the unique security key in a second data structure mechanism in the mobile device;~~

receiving a request to provide the unique security key for the mobile device to a service provider such that the service provider can provide a service to the mobile device based on the unique security key; and

approving the request to provide the unique security key to the service provider based on content of a list of ~~approved~~ service providers stored in a second data storage mechanism, ~~if a first condition is met, wherein the first condition is set by~~ ,

wherein the second data storage mechanism is directly accessible by the mobile device,;

~~and~~

~~providing the unique security key to the service provider, if the service provider is approved to receive the unique security key for the mobile device~~

wherein the content of the list of service providers is editable by a user of the mobile device by way of directly accessing the second data storage mechanism via the mobile device.

2. (Currently Amended) The method of claim 1, further comprising:

denying the request to provide the unique security key, if the service provider is not approved to receive the unique security key for the mobile device according to the content of the list of service providers stored in the second data storage mechanism.

3. (Canceled)

4. (Currently Amended) The method of claim 1, wherein the second data storage mechanism is a memory chip embedded in the mobile device.

5. (Currently Amended) The method of claim 1, wherein the second data storage mechanism is an identity module removably ~~for~~ insertable in the mobile device.

6. (Previously Provided) The method of claim 1, wherein the second data storage mechanism is a SIM card for the mobile device.

7. (Canceled)

8. (Currently Amended) The method of claim 1, wherein the unique ~~value~~ identification number is at least one of the mobile device's electronic serial number (ESN), international mobile equipment identity (IMEI) ~~and~~ or a phone number.

9-15 (Cancel)

16. (New) A secured communication system for a mobile communications network, the system comprising:

a logic unit for receiving a request to provide a security key to a mobile device connected to the mobile communications network;

a logic unit for generating a unique security key for the requesting mobile device in response to receiving a unique identification number from the mobile device;

a logic unit storing the unique security key in a first data storage mechanism in association with the unique identification number identifying the mobile device,

wherein the first data storage mechanism is accessible to a server system connected to the mobile device over a wide area communicatoin network and wherein the first data storage mechanism is not directly accessible by the mobile device;

a logic unit for receiving a request to provide the unique security key for the mobile device to a service provider such that the service provider can provide a service to the mobile device based on the unique security key; and

a logic unit for approving the request to provide the unique security key to the service provider based on content of a list of service providers stored in a second data storage mechanism,

wherein the second data storage mechanism is directly accessible by the mobile device,

wherein the content of the list of service providers is editable by a user of the mobile device by way of directly accessing the second data storage mechanism via the mobile device.

17. (New) The system of claim 16, further comprising:

denying the request to provide the unique security key, if the service provider is not approved to receive the unique security key for the mobile device according to the content of the list of service providers stored in the second data storage mechanism.

18. (New) The system of claim 16, wherein the second data storage mechanism is a memory chip embedded in the mobile device.

19. (New) The system of claim 16, wherein the second data storage mechanism is an identity module removably insertable in the mobile device.

20. (New) The system of claim 16, wherein the second data storage mechanism is a SIM card for the mobile device.